plans. However, based on the knowledge in the database, an application will provide an automatic conflict warning as a code is entered if an adverse situation exists.

The next three applications represent a more ambitious development effort by Mitretek. However, they will have a significant impact on the timing and quality of NPA relief planning efforts. At the present time, NPA relief planning is based on statistics compiled from data in the master database. These statistics are used in conjunction with maps of political boundaries to formulate a plan that balances code conservation with minimum impact on users. Variations of the plan are proposed and evaluated at public meetings and at regulatory commission hearings. There are two shortcomings of the present procedure:

1. The amount of time it takes to formulate a plan or a variation to a plan and compile the appropriate statistics.
2. The ability to convey the attributes of the plan in terms that all parties can understand and relate to.

Both of these shortcomings can be addressed through applications that links database information with geographic display techniques. Specifically, the ability to use color and three-dimensional rendering to show number density overlayed on political boundaries can greatly enhance the understanding of a proposed solution. The display would change in real-time as alternative assignments were considered, improving the efficiency of planning meetings. This data visualization technique has been used extensively in many industries and is supported by commercial, off-the-shelf software products, minimizing the development time required once the underlying data is available. A similar, parallel effort will develop measures of effectiveness for code assignment situations. These would be calculated form the statistics in the database and could include number balance, time to exhaust balance, community split ratios, etc. These measures would be calculated as assignments were proposed, allowing real time assessment of alternatives in a collaborative setting.

The final development effort is the application of advanced forecasting techniques to the number exhaust problem. This is also a highly rich field of study in other disciplines and a number of very powerful techniques have been developed (well beyond the linear projections historically used for exhaust planning). Mitretek has operational experience with moving average and exponential smoothing techniques as well as using filtering algorithms to remove seasonality and one time events from historical records. These techniques have been successfully applied to the forecasting of federal government traffic for use in large telecommunications procurements. The COCA database will contain a history of detailed information at the NXX level that has not been previously available. Coupled with better forecasts from tele-carriers as a result of Mitretek's neutrality, these techniques can reduce the surprises that result from each COCUS advancing the projected exhaust of NPAs from the previous COCUS and creating jeopardy situations. ■

9.2.2.5 Administrative Systems

Computer-based administrative systems will be extensively used to improve productivity and enable quick and accurate response to customer inquiries. E-mail hosts based on industry standards will be maintained at the main site. All Mitretek NANP Administration locations will utilize client software and access their mailboxes through dedicated circuits or dial-up connections.

In order to facilitate communications and coordination among the field sites and the main site, a Lotus Notes collaborative software system will be implemented. The main servers will be at the main site, with client software at the field sites. All NANP Administration personnel will interact with the database through then dedicated or dial-up connections described above. This type of collaborative interaction has been used successfully by Mitretek on major procurement projects for government customers.

Administrative systems will also be implemented to log and track events. All formal requests for resources will be logged and the completion dates noted. This will not only allow workload and performance measures to be derived, but will allow the status of events to be reported to customers. Summary statistics such as Web site hits and 800 call volumes will also be kept in the database for use in performance reporting. ■

9.2.2.6 System Development Schedule

Table 9-2 (which because of its size is included at the end of Section 9.2) lists the system components and functions sorted by their implementation phase. For NANPA functions, phase 0 is the end of the 60 day transition period, when the new NANPA resource administrator is performing the assignment functions. Phase 1 is complete at the end of the transition period for COCA functions (see Section 5). At this point, the system is fully operational. Phases 2, 3, and 4 constitute three six month periods of additional development to introduce more advanced functions and applications into the system. Phase 2 will add automatic publishing from the COCA databases to the internal Web site, resulting in workload savings for the COCA function and reducing the chances of input error on the Web site. Phase 3 adds two important applications designed to aid the COCA and the NPA relief planning staff. The first of these is automatic conflict warning if a code is entered that is infeasible due to equipment restrictions, dialing plan conflicts, or other criteria that would preclude assignment. This reduces the manual labor of the COCA staff in searching for such conflicts. The second application is the visualization of code utilization geographically. As discussed above, this powerful display can show the results of tentative code assignments during the planning of an NPA split.

Phase 4 implements the unlimited access to the NANP Administration internal network using Web browser technology over the Internet. This will only be performed if the supporting security technology (public key encryption and digital certificates) is available in the commercial marketplace. In addition, two advanced applications will become operational. The advanced forecasting system, operating at the NXX level and rolling up to the NPA level, will provide a more accurate estimate of exhaust dates than ever before. The alternative evaluation system will augment the data visualization system in providing measures of effectiveness for NPA splits and in providing initial solutions based on objective criteria. ■

Table 9-1 System Components - Sorted by Component

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
1	NANPA Resource Database	Hold NPA-level assignment data for 12 resources	NT 4.0, SQL Server, ODBC	User & Group Permissions	0	N/A
2	COCA Database	Hold NXX-level assignment data, hold line-level data	UNIX, Oracle, ODBC	User & Group Permissions	N/A	1
3.1	Internal Web Site	Internal Manual Update	NT 4.0/IIS	Password	0	1
3.2	Internal Web Site	Publishing from DB	NT 4.0/IIS, SQL Server	User & Group Permissions	1	2
3.3	Internal Web Site	DB Query via Web browser	NT 4.0/IIS, SQL Server	Authentication, User & Group Permissions	4	4
3.4	Internal Web Site	DB Update via Web browser	NT 4.0/IIS, SQL Server	Authentication, User & Group Permissions	4	4
4	External Web Site	Publishing from Internal Web Site	NT 4.0/IIS	None	0	1
5.1	Applications	Report Generation	MS Access, VB5.0, Stored Procedures	User & Group Permissions	0	1
5.2	Applications	Conflict Warning	VB5.0, VC++, C++	User & Group Permissions	N/A	3
5.3	Applications	Forecasting	VB5.0, VC++, C++	User & Group Permissions	N/A	4
5.4	Applications	Alternative Evaluation	VB5.0, VC++, C++	User & Group Permissions	N/A	4
5.5	Applications	Data Visualization	GIS	User & Group Permissions	N/A	3
6.1	NANPA Resource Workstation	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.2	NANPA Resource Workstation	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.3	NANPA Resource Workstation	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.4	NANPA Resource Workstation	Manual Internal Web Site Update	Windows 95, MS Access, ODBC, Web Browser	Password	0	N/A
6.5	NANPA Resource Workstation	Publishing from DB	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	N/A
6.6	NANPA Resource Workstation	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	4	N/A
6.7	NANPA Resource Workstation	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	4	N/A
7.1	COCA Workstation	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1

Table 9-1 (Continued)

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
7.2	COCA Workstation	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1
7.3	COCA Workstation	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1
7.4	COCA Workstation	Manual Internal Web Site Update	Windows 95, MS Access, ODBC, Web Browser	Password	N/A	1
7.5	COCA Workstation	Publishing from DB	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	2
7.6	COCA Workstation	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	N/A	4
7.7	COCA Workstation	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	N/A	4
7.8	COCA Workstation	Applications I	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	3
7.9	COCA Workstation	Applications II	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	4
8.1	Other Workstation	DB Query (Restricted)	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	1
8.2	Other Workstation	Web browsing	Windows 95, MS Access, ODBC, Web Browser	None	0	1
9	Security Boundary	Authentication	UNIX, Firewall	Secure ID or PKE	N/A	1
10.1	Remote Workstations	Authentication	Windows 95, MS Access, ODBC, Web Browser	Secure ID or PKE	1	1
10.2	Remote Workstations	Web browsing	Windows 95, MS Access, ODBC, Web Browser	None	1	1
10.3	Remote Workstations	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1
10.4	Remote Workstations	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1
10.5	Remote Workstations	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1

Table 9-1 (Concluded)

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
10.6	Remote Workstations	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	4	4
10.7	Remote Workstations	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	4	4
11.1	RDBS/BRIDS	Access	Windows 95, MS Access	None	0	1
11.2	RDBS/BRIDS	Update	Windows 95, MS Access	None	N/A	1

Table 9-2. System Components - Sorted by Implementation Phase

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
1	NANPA Resource Database	Hold NPA-level assignment data for 12 resources	NT 4.0, SQL Server, ODBC	User & Group Permissions	0	N/A
6.1	NANPA Resource Workstation	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.2	NANPA Resource Workstation	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.3	NANPA Resource Workstation	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	N/A
6.4	NANPA Resource Workstation	Manual Internal Web Site Update	Windows 95, MS Access, ODBC, Web Browser	Password	0	N/A
3.1	Internal Web Site	Internal Manual Update	NT 4.0/IIS	Password	0	1
4	External Web Site	Publishing from Internal Web Site	NT 4.0/IIS	None	0	1
5.1	Applications	Report Generation	MS Access, VB5.0, Stored Procedures	User & Group Permissions	0	1
8.1	Other Workstation	DB Query (Restricted)	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	0	1
8.2	Other Workstation	Web browsing	Windows 95, MS Access, ODBC, Web Browser	None	0	1
11.1	RDBS/BRIDS	Access	Windows 95, MS Access	None	0	1
2	COCA Database	Hold NXX-level assignment data, hold line-level data	UNIX, Oracle, ODBC	User & Group Permissions	N/A	1
7.1	COCA Workstation	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1
7.2	COCA Workstation	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1
7.3	COCA Workstation	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	1
7.4	COCA Workstation	Manual Internal Web Site Update	Windows 95, MS Access, ODBC, Web Browser	Password	N/A	1
9	Security Boundary	Authentication	UNIX, Firewall	Secure ID or PKE	N/A	1
11.2	RDBS/BRIDS	Update	Windows 95, MS Access	None	N/A	1
6.5	NANPA Resource Workstation	Publishing from DB	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	N/A

Table 9-2 (Continued)

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
10.1	Remote Workstations	Authentication	Windows 95, MS Access, ODBC, Web Browser	Secure ID or PKE	1	1
10.2	Remote Workstations	Web browsing	Windows 95, MS Access, ODBC, Web Browser	None	1	1
10.3	Remote Workstations	DB Query	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1
10.4	Remote Workstations	DB Update	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1
10.5	Remote Workstations	Report Generation	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	1	1
3.2	Internal Web Site	Publishing from DB	NT 4.0/IIS, SQL Server	User & Group Permissions	1	2
7.5	COCA Workstation	Publishing from DB	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	2
5.5	Applications	Data Visualization	GIS	User & Group Permissions	N/A	3
5.2	Applications	Conflict Warning	VB5.0, VC++, C++	User & Group Permissions	N/A	3
7.8	COCA Workstation	Applications I	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	3
6.6	NANPA Resource Workstation	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	4	N/A
6.7	NANPA Resource Workstation	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	4	N/A
7.6	COCA Workstation	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	N/A	4
7.7	COCA Workstation	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	Authentication, User & Group Permissions	N/A	4
3.3	Internal Web Site	DB Query via Web browser	NT 4.0/IIS, SQL Server	Authentication, User & Group Permissions	4	4
3.4	Internal Web Site	DB Update via Web browser	NT 4.0/IIS, SQL Server	Authentication, User & Group Permissions	4	4
10.6	Remote Workstations	DB Query via Web browser	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	4	4

Table 9-2 (Concluded)

Number	Item	Function	Technology	Security	NANP Resource Phase	COCA Phase
10.7	Remote Workstations	DB Update via Web browser	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	4	4
5.3	Applications	Forecasting	VB5.0, VC++, C++	User & Group Permissions	N/A	4
5.4	Applications	Alternative Evaluation	VB5.0, VC++, C++	User & Group Permissions	N/A	4
7.9	COCA Workstation	Applications II	Windows 95, MS Access, ODBC, Web Browser	User & Group Permissions	N/A	4

9.3 Security Requirements

Mitretek has a long tradition of handling and storing extremely sensitive and proprietary information. We have handled both national security sensitive data, as well as proprietary commercial price and technical information. We have a Mitretek Security Department that provides building security, security procedures, and personnel clearances and security. We also have our InfoSec Committee which is responsible for approving the security design, implementation and procedures of all Mitretek computer and communications systems. Staff serving on the Mitretek InfoSec Committee also provide expert information security support to our clients such as the National Security Agency Trusted Products Program. All aspects of the proposed security approaches are based on established procedures and systems developed by these groups.

Proper Security Measures. Mitretek will provide proper security measures required for handling sensitive and proprietary carrier information. The Mitretek NANP Administration will, because of the fundamental nature of this activity, handle some of the more sensitive and proprietary information in the telecommunications industry. We are prepared to take on the associated responsibility for the proper and complete safeguarding of this information. Mitretek has and does handle some of the most sensitive national security, as well as price sensitive and technological proprietary information from the major telecommunications carriers.

Security Requirements

The nature of Mitretek' technical work often involves the use of sensitive or proprietary information obtained from industry, the U.S. government, or other governments. Because of that work, Mitretek developed security measures appropriate for projects involving the most sensitive information and systems in the world. Many security measures now common in industry, such as security firewalls, smartcard synchronized secure identification systems and internet electronic commerce applications, were first developed, prototyped or tested at Mitretek or its predecessor organization. Mitretek has procedures in place to guarantee physical, information, and personnel security.

Mitretek will bring these already-established procedures, policy and expertise to bear in its work as the new NANP Administration. Mitretek realizes that the success of this program will hinge upon the new NANP Administration receiving very proprietary data from potentially competing segments and entities in a highly competitive industry. We have enclosed our Security Manual as an appendix to this response, and is willing to discuss and review its security procedures with any customer at any time.

Secured Work Area with Limited Access. Mitretek will provide a secured work area with limited access for all NANP Administration activities.

Mitretek sites have physical security measures in place that are appropriate to the nature of the project and information being handled at the site. Our McLean facilities, which holds an industrial security (i.e., code 7L030 for "Top Secret" and "Top Secret Storage") facilities clearance, has in place, for example, a number of security features. Each entrance and exit to the building is monitored by a camera 24 hours a day seven days a week. The building has one or more security guards on active patrol around the building 24 hours a day seven days a week. During extended business hours (5:00 AM - 6:00 PM five days a week) the entrances and exits to the building are staffed with trained security guards who grant access to the building under two conditions, the person entering the building has a current Mitretek picture identification badge or the person is personally authorized and escorted by a person with a current Mitretek picture identification badge. All employees must wear their Mitretek current picture identification badge in plain sight while in Mitretek facilities. Visitors to the Mitretek site are given escorted visitors badges and must be accompanied by someone with a current picture identification badge or may be given a one-day unescorted visitors badge with prior written authorization.

During other than extended business hours admittance can only be gained with a current Mitretek picture identification badge and personal identification number (PIN) through two-door access under the observation of cameras that are manned 24 hours a day seven days a week.

Additionally, all NANP Administration, at McLean and other facilities, will be located within a secure perimeter with access provided only through individual badge readers.

The secure perimeters will be established inside of the Mitretek facilities in addition to building access discussed above.

Secured Record Retention. Mitretek will provide secured record retention. Mitretek has specific policies and procedures for secured record retention. Paper copies of sensitive and proprietary records are clearly marked as such, and are secured in tamperproof fireproof file cabinet safes, which are approved for storage of information classified at the Top Secret level. Each workspace that contains safes has a safe closure log, the last person leaving the workspace at the end of a workday must physically check that each safe is locked and visually inspect no workspace has sensitive or proprietary records left out of the safe. Paper copies of secure information are assigned a specific lifespan according to the wishes of the owner. NANP Administration files will be maintained in tamperproof fireproof storage for the duration of Mitretek's tenure as NANP Administration in accordance with NANC directives.

Computer System Security. Mitretek will provide secured computer systems for processing of all NANP Administration data, including proprietary information.

Security Measures Against Internal Disclosure. As described in Section 9.2, all proprietary data is resident in databases that are connected to the NANP Administration internal network. This network is physically contained within space controlled for access only by NANP Administration personnel and authorized Mitretek management and support personnel (that is, the internal network is inside the NANP Administration secured perimeter). It will not be accessible to the general Mitretek population. In addition, database tables have read and write privileges assigned by user ID and password. Access to proprietary data will be assigned to specific personnel only on a need-to-know basis.

Security Measures Against External Disclosure. This information is presented as part of the information architecture section but is repeated here for emphasis and completeness. The security boundary is the only connection point between the NANP Administration internal network and the outside world. All NANP Administration electronic data, including proprietary data, is contained in databases connected to the internal network. The security boundary allows authorized users (e.g., NANP Administration personnel remote from the main site) to identify themselves absolutely and be connected to the internal network. Authorized users may then log onto the databases with their IDs and have the same privileges as if they were on the internal network.

The security boundary computer will be a Sun Microsystems SPARC 20 running the Solaris operating system, FireWall-1 security software from Checkpoint Software Technologies, and SecurID software from Security Dynamics, Inc. Access into the security boundary computer is through a bank of dial-in modems initially operating at 28.8 kb/s, over dedicated circuits operating at 64 kbps, or over the Internet. The boundary computer will be configured to allow users connecting over the Internet to have unlimited access to the external Web server, but no access to any internal NANP Administration resources. Upon connection through the modems or the dedicated circuits, the user is presented with a connection screen and must comply with the requirements of the security boundary computer to gain access to the internal network.

The initial technology that will be used for the security boundary is the SecurID technology from Security Dynamics. This method combines a smart card carried by the remote user with a password for that user. The card generates a random number each minute. The user types in his ID, a password, and the number on the card. The security boundary is also generating the same numbers as the user's card and associating them with the user's ID and password. If the user-provided password and number do not match the security machine's, then the user is rejected. This method protects against interception of the user's password and later unauthorized entry into the system. The security boundary also protects any internal systems from access by users of the external Web site.

A future implementation of the security boundary will use a secure Internet gateway in place of the dial-in modems. This gateway will employ a digital signature authentication system based on a nationally recognized certification authority. This will allow not only NANP Administration personnel to be identified, but will allow code requester companies to be certified for direct submission of electronic code requests to the NANP

Administration. This option will be implemented when the certification infrastructure is publicly available.

Disaster Recovery Plans and Procedures. Mitretek will provide disaster recovery plans and procedures. The Disaster Recovery Plan provides a blueprint for the provision of comparable NANP Administration services in an alternate site in the event the permanent facility is disabled for whatever reason. The detailed Plan will be developed in the course of the transition and addresses the following:

- Communications line outages
- Local area network failure
- Power failure
- Fire, flooding, and natural disaster
- Anticipated effect on service
- Notification and evaluation procedures
- Alternative procedures
- Status reporting procedures
- "Normal" service restoration procedures
- Post-crisis evaluation

Security Requirements

A detailed description of Mitretek's approach to disaster and service maintenance will be made to the NANC following development of the plan. The heart of the Mitretek Plan will be to protect the data resident in the master databases and the Web site, and be able to reconstitute normal operations at an alternate site in 24 to 36 hours. The alternate site will have the requisite computer and communications facilities, including security facilities, to sustain operations. The backup strategy will be based on and follow the normal Mitretek Computer Center (MTCC) procedures as described below.

The MTCC is able to reconstruct databases and corporate systems from backups by implementing hot and cold backup schema with archive logging, rotating tapes off-site, and utilizing technologically current backup software. Automated hot (daily) and cold (weekly) comprehensive backups are performed on all corporate systems for user file restores and disaster recovery events. The MTCC adheres to the industry standard GFS rotation schema in which daily and weekly backups are retired after a full accounting month, and monthly tapes are recycled annually. Tapes are sent to an authorized off-site storage facility in case of disaster recovery.

The MTCC employs state-of-the-art backup software which allows operations to monitor every facet of backup and archival storage, ensuring complete data integrity. An Uninterrupted Power Source system in the computer center guarantees critical applications and backups are unaffected by power failures and power surges. Providing for data recovery and system integrity in disastrous situations is the main goal of the Mitretek Computer Center. ■

9.4 Staffing Requirements

Mitretek recognizes the importance of the effective and efficient administration of the NANP to the telecommunications industry and the NANP participating countries. Mitretek brings the appropriate staff levels and skills required for NANP administration in a changing telecommunications industry and market. Mitretek offers the fresh, innovative staff and organization required for implementing the new NANP model as defined by the FCC and the NANC. Mitretek has identified and committed key personnel resources to be dedicated to the successful implementation and operation of the Mitretek NANP Administration. Additionally, Mitretek has engaged an executive search firm to seek and hire additional NANPA and COCA experienced staff and managers. This search, presented later in this section, has already yielded staff that have been hired by Mitretek and staff who are prepared to continue employment discussions if we are successful in our NANP Administration bid. Staffing levels in the new Mitretek NANP Administration will be appropriate to ensure that we effectively and efficiently perform all functions identified in the NANC Requirements Document. The Mitretek staffing proposal provides levels and quality of staff to ensure high-quality, timely responses to the requirements and to industry.

All Mitretek NANP Administration staff will be available during normal business hours as discussed in Section 9.1. However, as circumstances warrant, Mitretek NANP Administration staff will be available at all times to meet the needs of the industry and the

NANC. Mitretek has elected to establish five NANP locations—McLean, Virginia; Atlanta, Georgia; Chicago, Illinois; Denver, Colorado; and San Francisco, California. Mitretek staff will be available to travel, in order to meet all NANP needs of the industry (e.g., INC, seminars, NPA relief activities) and the NANC. The Mitretek staff possess the attributes required to perform the functions of the new NANP Administration as described in the Requirements Document. Mitretek proposed staffing profiles and levels are presented as a function of location, position level, and responsibility. ■

9.4.1 NANP Administration Staff Levels and Profiles

Staffing levels and profiles for the Mitretek NANP Administration are now presented. The Mitretek staffing plan is derived from the proposed organizational structure presented in Section 9.5. (For ease of understanding Section 9.4, we suggest that the reader examine Section 9.5 before continuing.) In determining staffing levels, Mitretek conducted a complete and thorough analysis of the number of numbering requests and NPA relief planning activities, as well as the organizational analysis presented in Section 9.5. We carefully identified and estimated the time required to perform each step of all NANP and COCA functions. Based on a thorough analysis of the data available, as well as consultation with numbering plan administrators, code administrators, and NPA relief planners, [redacted]

[redacted]

[redacted]

A complete enumeration of staffing levels by position and organizational component is presented in Figure 9-7. A complete set of detailed position descriptions is provided in Section 3.1. A discussion of Mitretek staff position levels is presented in Section 3.1; position descriptions are found in Appendix J. ■

9.4.2 Staffing the NANP Administration

The Mitretek staffing approach recognizes and addresses the need for staff with critical numbering plan and code administration experiences. Senior, experienced numbering plan and CO code administration professionals have already joined the Mitretek NANP team.

Staffing Requirements

The Mitretek staffing plan also recognizes that the successful NANP Administration of the future will require experiences beyond that of the NANPA and COCA base, including:

[redacted]

- Experience in operating in difficult roles requiring competitively-neutral and technology-neutral attributes
- Experience in managing proprietary data and competitively sensitive information
- Experience in sophisticated statistical data reduction and analysis, with the knowledge and initiative to apply such techniques proactively prior to the onset of problems
- Experience in providing defensible forecasts and sophisticated analytic solutions, again with the knowledge and initiative to apply such techniques proactively prior to the onset of problems
- Experience in developing and operating the modern computer, database, and communications systems required for such sophisticated data analysis and quantitative analysis
- Experience in considering difficult and complex problems in the framework of a new telecommunications industry and market models
- Experience in appropriate re-engineering of mission-critical operations to adapt to changing conditions and requirements

In order to staff the Mitretek NANP Administration in a responsive and timely manner, we have already implemented a three-pronged approach to staffing:

1. Identify and retain experienced numbering plan professionals
2. Dedicate existing Mitretek staff with telecommunications experiences beyond that of the current NANPA base